

**Yee &
Associates, P.C.**

13760 Noel Road
Suite 900
Dallas, Texas 75240

Main No. (972) 367-2001
Facsimile (972) 367-2008

RECEIVED
CENTRAL FAX CENTER

Facsimile Cover Sheet

OCT 12 2004

To: Commissioner for Patents for Examiner Michael R. Vaughan Group Art Unit 2131	Facsimile No.: 703/872-9306
From: Amelia Turner Legal Assistant to Stephen R. Tkacs	No. of Pages Including Cover Sheet: 30
Message: Transmitted herewith: <ul style="list-style-type: none">• Transmittal Document; and• Appeal Brief.	
Re: Application No. 09/584,605 Attorney Docket No: DE9-1999-0058	
Date: Tuesday, October 12, 2004	
Please contact us at (972) 367-2001 if you do not receive all pages indicated above or experience any difficulty in receiving this facsimile.	<i>This Facsimile is intended only for the use of the addressee and, if the addressee is a client or their agent, contains privileged and confidential information. If you are not the intended recipient of this facsimile, you have received this facsimile inadvertently and in error. Any review, dissemination, distribution, or copying is strictly prohibited. If you received this facsimile in error, please notify us by telephone and return the facsimile to us immediately.</i>

**PLEASE CONFIRM RECEIPT OF THIS TRANSMISSION BY
FAXING A CONFIRMATION TO 972-367-2008.**

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

RECEIVED
CENTRAL FAX CENTER
OCT 12 2004In re application of: **Bendel et al.**Serial No.: **09/584,605**Filed: **May 31, 2000**For: **Method and Apparatus for
Controlling Access to the Contents of
Web Pages by Using a Mobile Security
Module****36736**PATENT TRADEMARK OFFICE
CUSTOMER NUMBER§
§
§
§
§
§Group Art Unit: **2131**Examiner: **Vaughan, Michael R.**Attorney Docket No.: **DE9-1999-0058**Certificate of Transmission Under 37 C.F.R. § 1.8(a)

I hereby certify this correspondence is being transmitted via facsimile to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, facsimile number (703) 872-9306 on October 12, 2004.

By:


Amelia C. TurnerTRANSMITTAL DOCUMENTCommissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

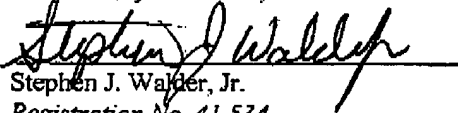
Sir:

TRANSMITTED HERewith:

- Appeal Brief (37 C.F.R. 41.37).

A fee of \$340.00 is required for filing an Appeal Brief. Please charge this fee to IBM Corporation Deposit Account No. 09-0461. No additional fees are believed to be necessary. If, however, any additional fees are required, I authorize the Commissioner to charge these fees which may be required to IBM Corporation Deposit Account No. 09-0461. No extension of time is believed to be necessary. If, however, an extension of time is required, the extension is requested, and I authorize the Commissioner to charge any fees for this extension to IBM Corporation Deposit Account No. 09-0461.

Respectfully submitted,


Stephen J. Walder, Jr.

Registration No. 41,534

Duke W. Yee

Registration No. 34,285

YEE & ASSOCIATES, P.C.

P.O. Box 802333

Dallas, Texas 75380

(972) 367-2001

ATTORNEYS FOR APPLICANTS

Docket No. DE9-1999-0058

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: **Bendel et al.**Serial No.: **09/584,605**Filed: **May 31, 2000**For: **Method and Apparatus for
Controlling Access to the Contents of
Web Pages by Using a Mobile Security
Module**§
§
§
§
§
§
§Group Art Unit: **2131**Examiner: **Vaughan, Michael R.**RECEIVED
CENTRAL FAX CENTER

OCT 12 2004

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450Certificate of Transmission Under 37 C.F.R. § 1.8(a)I hereby certify this correspondence is being transmitted via
facsimile to the Commissioner for Patents, P.O. Box 1450,
Alexandria, VA 22313-1450, facsimile number (703) 872-9306,
on 10.12.04

By:


Amelia C. Turner

APPEAL BRIEF (37 C.F.R. 41.37)

This brief is in furtherance of the Notice of Appeal, filed in this case on August 11, 2004.

The fees required under § 41.20(B)(2), and any required petition for extension of time for filing this
brief and fees therefore, are dealt with in the accompanying TRANSMITTAL OF APPEAL
BRIEF.(Appeal Brief Page 1 of 28)
Bendel et al. - 09/584,605

REAL PARTY IN INTEREST

The real party in interest in this appeal is the following party: International Business Machines Corporation.

RELATED APPEALS AND INTERFERENCES

With respect to other appeals or interferences that will directly affect, or be directly affected by, or have a bearing on the Board's decision in the pending appeal, there are no such appeals or interferences.

STATUS OF CLAIMS

A. TOTAL NUMBER OF CLAIMS IN APPLICATION

Claims in the application are: 1-5, 7-9, 12-14, and 23-33

B. STATUS OF ALL THE CLAIMS IN APPLICATION

1. Claims canceled: 6, 10, 11, and 15-22
2. Claims withdrawn from consideration but not canceled: NONE
3. Claims pending: 1-5, 7-9, 12-14, and 23-33
4. Claims allowed: NONE
5. Claims objected to: NONE
6. Claims rejected: 1-5, 7-9, 12-14, and 23-33

C. CLAIMS ON APPEAL

The claims on appeal are: 1-5, 7-9, 12-14, and 23-33

STATUS OF AMENDMENTS

There are no amendments to the claims after final rejection. An amendment to the specification after final rejection was entered, as specified in the Advisory Action dated August 17, 2004.

SUMMARY OF CLAIMED SUBJECT MATTER

Independent claim 1:

The present invention provides a method for controlling access to protected access on a server where a server 107, client 101, a reader 103 for a mobile security module, a security module 105 having at least one protected area for storing a key, and a data line for communications between the client and the server are present. See specification, page 6, line 5, to page 7, line 16; **Figure 1**. The method is characterized by the steps of sending to the server a request to call up protected-access content, sending from the server to the client an authentication module to be run in the client, and execution of an authentication protocol for authenticating the mobile security module. See specification, page 8, line 1, to page 10, line 4; **Figure 2**. The method is also characterized by the steps of adding a session ID to the request, sending the new request to the server, and checking the session ID in the request to see if it is recorded in the server. See specification, page 10, line 5, to page 11, line 2; **Figure 2**. The method is further characterized by the steps of processing the content requested for transmission and searching the contents for further links to protected-access content, adding the session ID to the links, and sending the content to the client. See specification, page 11, lines 3-13; **Figure 2**.

Independent claims 23, 27, and 33:

In addition to the above, the present invention may also present a method, apparatus, and computer program product, in a client, for sending a request for protected content to a server, receiving an authentication applet and a random number from the server, wherein the random number is generated at the server, and executing the authentication applet. See specification, page 8, line 1, to page 10, line 4; **Figure 2**. The authentication applet sends the random number to a mobile security module. The mobile security module includes a cryptographic key and generates a cryptographic signature based on the key and the random number. See specification, page 8, line 17, to page 9, line 3; **Figure 2**. The authentication applet then receives the cryptographic signature from the mobile security module and sends the cryptographic signature to the server. See specification, page 9, lines 4 and 5; **Figure 2**. Responsive to the server

authenticating the cryptographic signature, the client receives a session identifier from the server. See specification, page 9, line 6, to page 10, line 4; **Figure 2**.

The means recited in independent claim 27, as well as dependent claims 28-32, may be data processing hardware within client 101 operating under control of software performing the steps described in the specification at page 7, line 17, to page 12, line 7. A person having ordinary skill in the art would be able to derive computer instructions on a computer readable medium given **Figure 2** and the corresponding description at page 7, line 17, to page 12, line 7, without undue experimentation.

GROUND OF REJECTION TO BE REVIEWED ON APPEAL

The grounds of rejection on appeal are as follows:

Claims 23-32 are rejected under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claims 1, 2, and 14 are rejected under 35 U.S.C. § 102 as being anticipated by *Handel et al.* (U.S. Patent No. 6,195,651);

Claims 23-30, 32, and 33 are rejected under 35 U.S.C. § 102 as being anticipated by *Laursen et al.* (U.S. Patent No. 6,065,120);

Claims 3, 4, and 7-9 are rejected under 35 U.S.C. § 103 as being unpatentable over *Handel* in view of *Hopkins* (U.S. Patent No. 5,757,918);

Claims 5, 12, and 13 is rejected under 35 U.S.C. § 103 as being unpatentable over *Handel* in view of *Lin et al.* (U.S. Patent No. 6,052,785); and,

Claim 31 is rejected under 35 U.S.C. § 103 as being unpatentable over *Laursen* in view of *Handel*.

ARGUMENT

I. 35 U.S.C. § 112, Second Paragraph, Alleged Indefiniteness of Claims 23-32

The Final Office Action rejects claims 23-32 under 35 U.S.C. § 112, second paragraph, as allegedly being indefinite for failing to particularly point out and distinctly claim the subject matter, which applicants regard as the invention. This rejection is respectfully traversed.

The Office Action alleges that independent claims 23 and 27 do not recite whether the client, the authentication applet, or neither is performing the step of "receiving a session identifier from the server." Claims 23 and 27 clearly recite a method and an apparatus in a client. Nonetheless, the claims are definite without having to recite the specific structure that performs the recited functions. Perhaps the step or function in question is broader than it would be if it explicitly recited the structure performing the function; however, there is no requirement under 35 U.S.C. § 112, second paragraph, that method claims and means-plus-function claims recite specific structure limitations to be definite. Breadth is a consideration for 35 U.S.C. §§ 102 and 103, not 35 U.S.C. § 112.

Therefore, Appellants respectfully request that the rejection of claims 23-32 under 35 U.S.C. § 112, second paragraph, not be sustained.

II. 35 U.S.C. § 102, Alleged Anticipation of Claims 1, 2, and 14

The Final Office Action rejects claims 1, 2, and 14 under 35 U.S.C. § 102 as being allegedly anticipated by *Handel et al.* (U.S. Patent No. 6,195,651). This rejection is respectfully traversed.

Handel teaches a system, method, and article of manufacture for a tuned user application experience. A user's interface to a particular application program is modified by obtaining user profile information. Content is parsed and the parsed content is matched to the user profile information. Matches are presented in a format based on information in the user's profile. See *Handel*, Abstract; col. 1, lines 53-61.

In contradistinction, the present invention provides a mechanism for managing controlled access to protected content on a server using a mobile security module. The mobile security module authenticates with an authentication module. A session identifier (ID) is generated responsive to the mobile security module successfully authenticating with the authentication

module.

The Office Action alleges that *Handel* teaches adding a session ID to the request if the authentication was successful and cites col. 34, lines 63-66, as allegedly teaching this features.

The cited portion of *Handel* states:

Personal Profile and Services Ubiquity

This system provides one central storage place for a person's profile. This storage place is a server available through the public Internet, accessible by any device that is connected to the Internet and has appropriate access. Because of the ubiquitous accessibility of the profile, numerous access devices can be used to customize services for the user based on his profile. For example, a merchant's web site can use this profile to provide personalized content to the user. A Personal Digital Assistant (PDA) with Internet access can synchronize the person's calendar, email, contact list, task list and notes on the PDA with the version stored in the Internet site. This enables the person to only have to maintain one version of this data in order to have it available whenever it is needed and in whatever formats it is needed.

FIG. 17 presents the detailed logic associated with the many different methods for accessing this centrally stored profile. The profile database 1710 is the central storage place for the users' profile information. The profile gateway server 1720 receives all requests for profile information, whether from the user himself or merchants trying to provide a service to the user. The profile gateway server is responsible for ensuring that information is only given out when the profile owner specifically grants permission. Any device that can access the public Internet 1730 over TCP/IP (a standard network communications protocol) is able to request information from the profile database via intelligent HTTP requests. Consumers will be able to gain access to services from devices such as their televisions 1740, mobile phones, Smart Cards, gas meters, water meters, kitchen appliances, security systems, desktop computers, laptops, pocket organizers, PDAs, and their vehicles, among others. Likewise, merchants 1750 will be able to access those profiles (given permission from the consumer who owns each profile), and will be able to offer customized, personalized services to consumers because of this.

One possible use of the ubiquitous profile is for a hotel chain. A consumer can carry a Smart Card that holds a digital certificate uniquely identifying him. This Smart Card's digital certificate has been issued by the system and it recorded his profile information into the profile database. The consumer brings this card into a hotel chain and checks in. The hotel employee swipes

the Smart Card and the consumer enters his Pin number, unlocking the digital certificate. The certificate is sent to the profile gateway server (using a secure transmission protocol) and is authenticated. The hotel is then given access to a certain part of the consumer's profile that he has previously specified. The hotel can then retrieve all of the consumer's billing information as well as preferences for hotel room, etc. The hotel can also access the consumer's movie and dining preferences and offer customized menus for both of them. The hotel can offer to send an email to the consumer's spouse letting him/her know the person checked into the hotel and is safe. All transaction information can be uploaded to the consumer's profile after the hotel checks him in. This will allow partners of the hotel to utilize the information about the consumer that the hotel has gathered (again, given the consumer's permission).

Handel, col. 34, line 16, to col. 35, line 9. Neither the cited portion, nor any other portion of *Handel*, teaches adding a session ID to a request if a mobile security module successfully authenticates with an authentication module, as recited in claim 1. Rather, *Handel* merely teaches granting access to a user's profile at a hotel terminal if a smart card authenticates with the hotel terminal.

The Final Office Action argues that a session ID is something that uniquely identifies a session from other sessions and concludes that *Handel* teaches a session ID because *Handel* teaches a unique ID that identifies a "persona." The Final Office Action alleges that any combination of persona and merchant would dictate a different session ID. Applicants respectfully disagree. A combination of a persona and a merchant is only indicative of the persona and the merchant. For example, if a persona has thousands of sessions with the same merchant, there will still only be one combination of that persona and that merchant. Therefore, a combination of a persona and a merchant does not identify the session at all.

Furthermore, claim 1, for example, recites that the session ID is generated in the course of the communications between the authentication module and the server. Clearly, the persona and merchant of *Handel* are established prior to a communications session. While the Final Office Action appears to try to interpret the teachings of *Handel* to meet the limitation of a session ID, the Final Office Action does not provide any explanation as to how these teachings meet the claim as a whole.

Furthermore, the Final Office Action alleges that *Handel* teaches checking of the session ID in the request to see that it is recorded in the server and cites the same portion of the reference as allegedly teaching this feature. Neither the cited portion, nor any other portion of *Handel*, mentions checking whether a session ID is recorded in the server, because, as discussed above, *Handel* does not teach or fairly suggest generating a session ID responsive to a mobile security module successfully authenticating with an authentication module. With respect to the interpretation of the teachings of *Handel* discussed above, there is no teaching in *Handel* that a persona ID or a merchant ID is stored in a server.

Still further, the Final Office Action alleges that *Handel* teaches processing the content requested for transmission, searching the content for further links to other protected-access content, and adding the session ID to the identified links and cites the same portion reproduced above as teaching these features. Clearly, the cited portion fails to even mention searching for links to other protected-access content. The Final Office Action proffers no analysis as to why the cited portion of *Handel*, or any other portion, teaches the recited features, but rather baldly concludes that the features are somehow taught.

The applied reference fails to teach or suggest each and every claim limitation. Therefore, *Handel* does not anticipate claim 1. Since claims 2 and 14 depend from claim 1, the same distinctions between *Handel* and the invention recited in claim 1 apply for these claims. Additionally, claims 2 and 14 recite other additional combinations of features not suggested by the reference.

Furthermore, *Handel* does not teach, suggest, or give any incentive to make the needed changes to reach the presently claimed invention. *Handel* actually teaches away from the presently claimed invention because it teaches providing unrestricted access to an operator of a hotel terminal, upon successful authentication with a smart card, without generating a session ID, as opposed to restricting access to protected content using a session ID, as in the presently claimed invention. Absent the Office Action pointing out some teaching or incentive to implement *Handel* to generate a session ID responsive to successful authentication with a mobile security module, one of ordinary skill in the art would not be led to modify *Handel* to reach the present invention when the reference is examined as a whole. Absent some teaching, suggestion, or incentive to modify *Handel* in this manner, the presently claimed invention can be reached

only through an improper use of hindsight using Appellants' disclosure as a template to make the necessary changes to reach the claimed invention.

Therefore, Appellants respectfully request that the rejection of claims 1, 2, and 14 under 35 U.S.C. § 102 not be sustained.

III. 35 U.S.C. § 102, Alleged Anticipation of Claims 23-30, 32, and 33

The Office Action rejects claims 23-30, 32, and 33 under 35 U.S.C. § 102 as being allegedly anticipated by *Laurson* (U.S. Patent No. 6,065,120). This rejection is respectfully traversed.

Laurson teaches a system of self-authentication by authorized users of devices with limited computing power. Before the request is made, a client generates a non-repeatable number (C-nonce) so that the client may authenticate the server. See *Laurson*, col. 10, lines 18-62. Thus, in *Laurson* the client is authenticating the server, rather than the server authenticating the client. The client sends a session request to a server. The client may be a mobile device or cellular phone. See *Laurson*, col. 9, lines 55-64. The server responds with a session reply that includes a session ID, a session key, a non-repeatable number (C-nonce), and a cipher that represents the choice of encryption the server proposes. See *Laurson*, col. 11, line 43, to col. 12, line 44. Therefore, the server replies with a session ID well before authentication is complete. The client may then determine whether the non-repeatable number from the server is the same as the non-repeatable number originally generated by the client. If so, then the server authentication is successful. See *Laurson*, col. 12, lines 24-44.

The above-described process is used to authenticate a server from a computationally limited client device. *Laurson* does not teach a mobile security module or an authentication applet. The Final Office Action alleges that *Laurson* teaches a mobile security module at col. 12, lines 10-15 and 45-53. *Laurson* states:

When the client 170 receives the SP 176 from the server 172, it performs the step one server authentication, which is considered successful if Encry[sessionID, key, S-nonce, derivative, cipher] in the received SP 176 is decrypted successfully with the shared encrypt key. If the step one server authentication fails, the client 170 discards the SP 176 and a new session creation may be started over again. Upon the success of the step one server authentication, the client 170 proceeds with the step two server authentication;

namely the predetermined relationship between the C-nonce and the derivative thereof should hold for a successful step-two server authentication:

C-nonce=derivative-1

If the C-nonce derived from the SP 176 is the same as the C-nonce originally generated by the client, the step two server authentication is successful, hence the server 172 is considered authenticated, trusted from the viewpoint of the client, and the SP 176 is accepted as a valid message, which means that the client 170 then uses the session key and other information in the SP 176 for the session being created. Only with both successful steps of the server authentication, the client 170 marks the session as committed, which means that transactions can be conducted subsequently in the session, again only from the viewpoint of the client 170. If the predetermined relationship between the client nonce and the derivative thereof does not hold, the step two server authentication fails and the received SP 176 is discarded. The client 170 may abort the session creation process if no further SP's are received and pass both steps of the server authentication during the time period allowed for a session creation. To provide the server with means for reassuring the client authentication by itself through the client, a derivative of the S-nonce, similar to the derivative of the C-nonce, is generated.

The client 170 then sends the server 172 a SC 178 to complete the session creation process. The SC 178 comprises the following information:

SC={Encry[derivative]};

where the derivative is the client's response to the server nonce challenge, namely the result of the verification, the derivative is used by the server 172 for step two client authentication. Further it is noted that the SC 178 is an encrypted message, meaning that the client encrypts the information in the SC 178 according to either its own cipher or the server proposed cipher. Generally the client 170 encrypts the information in the SC 178 according to the server proposed cipher if it accepts the server proposed cipher, otherwise, it encrypts the SC according to its own cipher.

Laursen, col. 12, lines 10-59. There is no teaching whatsoever of sending, by an authentication applet, the random number to a mobile security module and receiving, by the authentication applet, the cryptographic signature from the mobile security module, as recited in claim 23, for example. The Office Action proffers no analysis as to why the teaching of a client authenticating a server, as taught in *Laursen*, somehow teaches sending a random number to a **mobile security module** or receiving a cryptographic signature from a **mobile security module**.

The Office Action alleges that *Laurson* teaches an authentication applet at col. 14, line 44. The referenced line of the *Laurson* patent does indeed use the word "applet." However, *Laurson* does not teach or suggest that the applet sends a random number to a mobile security module, receives a cryptographic signature from the mobile security module, or sends the cryptographic signature to a server. Rather the applet of *Laurson* is part of a user interface through which a user may access an account. The Office Action proffers no analysis as to why this is somehow equivalent to the features of claim 23, for instance.

Furthermore, as mentioned above, the server of *Laurson* provides a session ID to the client responsive to receiving a session request. The client then completes the session creation process if server authentication is successful. However, *Laurson* does not teach or fairly suggest that the client receives a session identifier from the server **responsive to the server authenticating the cryptographic signature**, as recited in claim 23, for example.

Consequently, the applied reference does not anticipate at least claim 23. Independent claims 27 and 33 recite subject matter addressed above with respect to claim 23 and are allowable for the same reasons. Since claims 24-26 and 28-32 depend from claims 23 and 27, the same distinctions between *Laurson* and the invention recited in claims 23 and 27 apply for these claims. In addition, claims 24-26 and 28-32 recite other combinations of features not suggested by the applied reference.

Therefore, Appellants respectfully request that the rejection of claims 23-30, 32, and 33 under 35 U.S.C. § 102 not be sustained.

III.A. 35 U.S.C. § 102, Alleged Anticipation of Claims 25, 26, 29, and 30

More particularly, with respect to claims 25 and 29, the Final Office Action alleges that *Laurson* teaches that the mobile security module generates a cryptographic signature based on an individual number at col. 10, lines 8-12 and 56. While the cited portion of *Laurson* does indeed teach a device ID, which may be interpreted as an individual number, *Laurson* does not teach that a mobile security module uses the device ID to generate a cryptographic signature. The Final Office Action does not point out where the reference teaches a cryptographic signature other than to cite a seemingly irrelevant portion of the reference, which makes no mention whatsoever of a cryptographic signature. Thus, the Final Office Action does not establish a

prima facie case of anticipation for claims 25 and 29.

The applied reference does not teach each and every claim limitation; therefore, *Laursen* does not anticipate claims 25 and 29. Since claims 26 and 30 depend from claims 25 and 29, respectively, the same distinctions between *Laursen* and the invention recited in claims 25 and 29 apply for these claims.

Therefore, Appellants respectfully request that the rejection of claims 25, 26, 29, and 30 under 35 U.S.C. § 102 not be sustained.

IV. 35 U.S.C. § 103, Alleged Obviousness of Claims 3, 4, and 7-9

The Final Office Action rejects claims 3, 4, and 7-9 under 35 U.S.C. § 103 as allegedly being unpatentable over *Handel* in view of *Hopkins* (U.S. Patent No. 5,757,918). This rejection is respectfully traversed.

Claims 3, 4, 7, 8, and 9 depend from claim 1 and are allowable at least for the reasons stated above with respect to claim 1. Additionally, claims 3, 4, 7, 8, and 9 recite other additional combinations of features not suggested by the reference. As stated above, *Handel* fails to teach or fairly suggest adding a session ID to a request if a mobile security module successfully authenticates with an authentication module, checking of the session ID in the request to see that it is recorded in the server, processing the content requested for transmission, searching the content for further links to other protected-access content, and adding the session ID to the identified links, as recited in claim 1.

Hopkins does teach verifying a smart card and the identity of a user of the smart card to gain access to a security device. However, *Hopkins* does not make up for the deficiencies of *Handel*. To the contrary, *Hopkins* actually teaches away from the presently claimed invention because it teaches verifying a user and/or authenticating a smart card in an **off-line** environment, as opposed to restricting access to protected content using a session ID, as in the presently claimed invention. Absent the Office Action pointing out some teaching or incentive to implement *Hopkins* to generate a session ID responsive to successful authentication with a mobile security module, one of ordinary skill in the art would not be led to combine *Handel* and *Hopkins* to reach the present invention when the prior art is examined as a whole. Absent some teaching, suggestion, or incentive to combine *Hopkins* with *Handel* in this manner, the presently

claimed invention can be reached only through an improper use of hindsight using Applicants' disclosure as a template to make the necessary changes to reach the claimed invention.

Therefore, Appellants respectfully request that the rejection of claims 3, 4, 7, 8, and 9 under 35 U.S.C. § 103 not be sustained.

V. 35 U.S.C. § 103, Alleged Obviousness of Claims 5, 12, and 13

The Final Office Action rejects claims 5, 12, and 13 under 35 U.S.C. § 103 as allegedly being unpatentable over *Handel* in view of *Lin et al.* (U.S. Patent No. 6,052,785). This rejection is respectfully traversed.

Claims 5, 12, and 13 depend from claim 1 and are allowable at least for the reasons stated above with respect to claim 1. Additionally, claims 5, 12, and 13 recite other additional combinations of features not suggested by the reference. *Lin* does generally teach secure socket layer (SSL) security protocol. However, *Lin* does not make up for the deficiencies of *Handel*. As stated above, *Handel* fails to teach or fairly suggest adding a session ID to a request if a mobile security module successfully authenticates with an authentication module, checking of the session ID in the request to see that it is recorded in the server, processing the content requested for transmission, searching the content for further links to other protected-access content, and adding the session ID to the identified links, as recited in claim 1. Merely combining the teachings of *Handel* with general teachings of SSL would not result in the present invention as recited in claims 5, 12, and 13.

Therefore, Appellants respectfully request that the rejection of claims 5, 12, and 13 under 35 U.S.C. § 103 not be sustained.

VI. 35 U.S.C. § 103, Alleged Obviousness of Claim 31

The Final Office Action rejects claim 31 under 35 U.S.C. § 103 as allegedly being unpatentable over *Laursen* in view of *Handel*. This rejection is respectfully traversed.

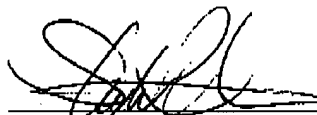
Claim 31 depends from claim 23 and is allowable at least for the reasons stated above with respect to claim 23. Additionally, claim 31 recites other additional combinations of features not suggested by the reference. *Handel* does generally teach a chip card and a chip card reader. However, *Handel* does not make up for the deficiencies of *Laursen*. As stated above, *Laursen*

fails to teach or fairly suggest an authentication applet that sends a random number to a mobile security module, receives a cryptographic signature from the mobile security module, and sends the cryptographic signature to a server, as recited in claim 23, for example. Merely combining the teachings of *Laurson* with general teachings of chip cards would not result in the present invention as recited in claim 31. Rather, a combination of *Laurson* and *Handel* would simply lead a person of ordinary skill in the art to replace the client of *Laurson*, which may be a mobile device or cellular telephone, with a chip card device.

Therefore, Appellants respectfully request that the rejection of claim 31 under 35 U.S.C. § 103 not be sustained.

CONCLUSION

In view of the above, Appellants respectfully submit that claims 1-5, 7-9, 12-14, and 23-33 are allowable over the cited prior art and that the application is in condition for allowance. Accordingly, Appellants respectfully requests the Board of Patent Appeals and Interferences to not sustain the rejections set forth in the Final Office Action.



Stephen R. Tkacs
Reg. No. 46,430
YEE & ASSOCIATES, P.C.
PO Box 802333
Dallas, TX 75380
(972) 367-2001